AO 91 (Rev. 01/09) Criminal Complaint

FILED
RICHARD W. NAGEL
CLERK OF COURT
2016 AUG -1 AM 10:59
U.S. DISTRICT COURT
SOUTHERN DIST OHIO
WEST DIV CINCINNATI

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

United States of America
v.
Carlos Ruiz-Rodriguez

Defendant

Case No. 1:16MJ-452

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date of ______ in the county of Hamilton in the Southern District of Ohio, the defendant violated 18 U. S. C. § 875(d), an offense described as follows:

Extortion through interstate communications.

This criminal complaint is based on these facts:

See attached Affidavit of S.A. Tae Dempsey.

☑ Continued on the attached sheet.

[signature]
Complainant's signature

Tae L. Dempsey, Special Agent FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 08/01/2016

Stephanie K. Bowman
Judge's signature

City and state: Cincinnati, OH

Hon. Stephanie K. Bowman, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF COMPLAINT

I, Tae L. Dempsey, a Special Agent with the Federal Bureau of Investigation, being duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent of the Federal Bureau of Investigation since September 2015, and am currently assigned to the Cincinnati Division. Prior to my employment at the Federal Bureau of Investigation, I was employed for five years as a Vice President and Information Security Officer at a major global bank in the Financial Services sector. While employed by the Federal Bureau of Investigation, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Bureau of Investigation and everyday work relating to conducting these types of investigations. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

2. This investigation pertains to the computer intrusion and theft of proprietary information from a Cincinnati-based company, followed by an extortion of that company, resulting in a $15,000 extortion payment and over $525,000 in exposed losses to the company. I make this affidavit in support of a Complaint and Arrest Warrant charging CARLOS RUIZ-RODRIGUEZ with extortion in violation of 18 U.S.C. § 875(d).

3. This affidavit is intended to show only that there is sufficient probable cause for the requested Complaint and Arrest Warrant and does not set forth all of my knowledge about this matter.

PERTINENT FEDERAL CRIMINAL STATUTES

4. 18 U.S.C. § 875(d) (extortion in interstate communications) states that it is a violation for any person to transmit in interstate commerce any communication containing any threat to injure the property or reputation of the addressee or of another, with the intent to extort any money or other things of value from any person, firm, association or corporation.

PROBABLE CAUSE

5. [redacted] located in Cincinnati, OH, is the corporate parent of [redacted].

6. Between November 2015 and January 2016, [redacted] received multiple extortion emails via the internet stating that if [redacted] did not pay a Bitcoin (BTC) ransom, then company schematics and client data would be released to the public. The extortion emails were sent on the following dates: 11/17/2015, 11/21/2015, 12/23/2015, 12/27/2015,

12/29/2015, 12/20/2015, and 1/7/2016. The emails used a technique and service to obscure the identity and true IP address of the sender.

7. During the above time period and in the extortion emails, the subject provided proof of compromise by means of attachments that contained [redacted] client data, [redacted] schematics, employee passwords, and knowledge of company internal communications.

8. [redacted] data was posted on an internet dark web forum called Hell Reloaded. The [redacted] data was posted the user named "ROR[RG]". The data was believed to have been first uploaded on January 7, 2016, followed by two larger data postings on January 9, 2016.

9. Shortly thereafter. [redacted] made two separate ransom payments on January 14, 2016 and January 21, 2016, totaling 36.60445829 BTC, or approximately [redacted] USD at the time, to the extortionist's Bitcoin account number. The subject did not contact anyone at [redacted] following the two payments.

10. CARLOS RUIZ-RODRIGUEZ had been employed at [redacted] for approximately two years as a work from home call center employee. He was terminated by [redacted] on [redacted], 2015 based on his attitude and a Better Business Bureau complaint against him. In his role at [redacted], RUIZ-RODRIGUEZ had access to the company's Internet-accessible customer service portal and therefore the personally identifiable information for certain clients.

11. An anonymous employee at [redacted] advised [redacted] management of a belief that the individual behind the extortion might have been RUIZ-RODRIGUEZ. The employee advised that another employee at [redacted] informed them that RUIZ-RODRIGUEZ had been talking about how he could sell the company's data and client information for a large sum of money and how this made RUIZ-RODRIGUEZ excited.

12. On January 20, 2016, [redacted], located in Cincinnati, OH, hired RUIZ-RODRIGUEZ as a customer service representative.

13. A confidential human source (CHS) employed at [redacted] advised [redacted] management that, in February 2016, the CHS had heard RUIZ-RODRIGUEZ talk about how he extorted his previous employer [redacted] for [redacted]. [redacted] never publically released the amount of the extortion payments.

14. While employed at [redacted], RUIZ-RODRIGUEZ had attempted to acquire the network administrator password from information technology department personnel, and on multiple occasions stated how the company would be easy to hack.

15. In July 2016, RUIZ-RODRIGUEZ described to the CHS that he identified employees at [redacted] who would have access to sensitive data. He then claimed that he obtained the schematics for the company's [redacted] products and also obtained customer information [redacted].

16. The CHS was able to observe RUIZ-RODRIGUEZ's personal laptop and the extortion emails that RUIZ-RODRIGUEZ sent to [redacted]. In meeting with RUIZ-RODRIGUEZ,

CHS also captured the Bitcoin wallet number that RUIZ-RODRIGUEZ had on his personal laptop. This Bitcoin account number matched the account number that was used in the [redacted] extortion.

TECHNICAL TERMS

17. Based on my training and experience, I use the following technical terms to convey the following meanings:

    a. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

CONCLUSION

18. Based on the forgoing, I believe that there is probable cause to show that CARLOS RUIZ-RODRIGUEZ has violated 18 U.S.C. 875 (extortion) from approximately November 2015 through January 2016.

REQUEST FOR SEALING

19. I further request that the Court order that all papers in support of this affidavit and Complaint be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise jeopardize the investigation.

Respectfully submitted,

Tae L. Dempsey
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me this 1 day of August 2016:

Stephanie K. Bowman

THE HONORABLE STEPHANIE K. BOWMAN
UNITED STATES MAGISTRATE JUDGE